Security Quickie 2-7-03: Working from Home

Connecting to your workplace network form home can be a great experience for some. A handy refrigerator, a quiet work area, and no pesky co-workers that watch you over your cubicle walls can certainly be thought of as a nice working environment. Of course, there are other benefits such as wearing fuzzy slippers, no one seeing your disarrayed hair and mismatched clothes, and not caring about those pop cans and potato chip bags strewn abound your desk. (Well, ok, I have seen pop-can pyramids at work. I suppose those people like the homelike atmosphere.) It's a setting that can leave you comfortable, efficient, and feeling safe. But when you connect from home, is the network as safe and cozy as you are? Here are some tips to help keep the state network secure when you work from home:

- Don't connect to another Internet Service Provider or network while connected to the state network. (Split tunneling, for example.) Unauthorized persons could get to the state network through your system when you simultaneously connect to both the state and a different ISP.
- Use good passwords and change them regularly, and use current anti-virus and firewall programs. If a virus or Trojan horse gets into your home system, it may later infect the state network when you do connect.
- If possible, arrange to have your home system security managed by your department, and at the very least follow all the security policies and procedures at home that you follow at work. Your department may be able to supply you with anti-virus and other protective measures as well.
- Protect any government data on your home system. Don't allow any service company or any unauthorized persons to access to that data; remove state information from the system before it is serviced, and use things like folder or disk encryption to protect state information on a day-to-day basis.
- Remote Control and File Sharing products are dangerous for systems that have state data. Don't use RC or P2P tools (GoToMyPC, Gnutella, Kazaa, etc.) on systems that have state information because unauthorized people could easily gain access to that data. Even if that data is encrypted, sharing programs can still grab it and send it somewhere else, to be cracked at a hacker's leisure.
- Wireless can be cool, but very insecure. Most wireless systems have lots of holes, so either highly secure it, or don't use it.
- If you connect to the state network from home, you have a responsibility to keep your home system secure. Home systems are far easier to compromise via the Internet or with user installations because they usually do not have the same security posture as workplace systems. Most home users are also unaware of many of the security risks associated with home systems, yet whenever home users connect to work systems, they impose the security issues of their home systems on the state network. Be safe, keep your home PC secure and protect your own system as well as the state's network.